

Εργαστήριο Δικτύων Υπολογιστών

Εργαστηριακή ασκηση **1**

Κουστένης Χρίστος | el20227 | 16/02/2024

PC name: RB19

# Άσκηση 1: Γνωριμία με το περιβάλλον εργασίας

### 1.1

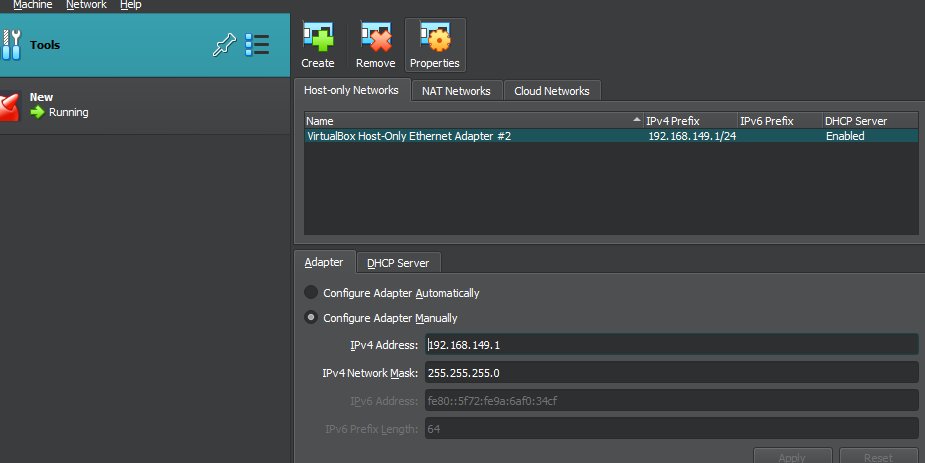
IPv4 address : 192.168.149.1

### 1.2

Subnet Mask: 255.255.255.0

### 1.3

Ναι, είναι.

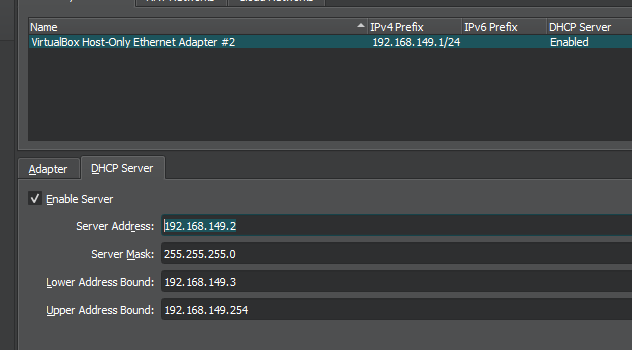


### 1.4

Server Address : 192.168.149.2

Lower Address Bound : 192.168.149.3

Upper Address Bound : 192.168.149.254



### 1.5

Εμφανίζεται η προτροπή lab@PC:~ %



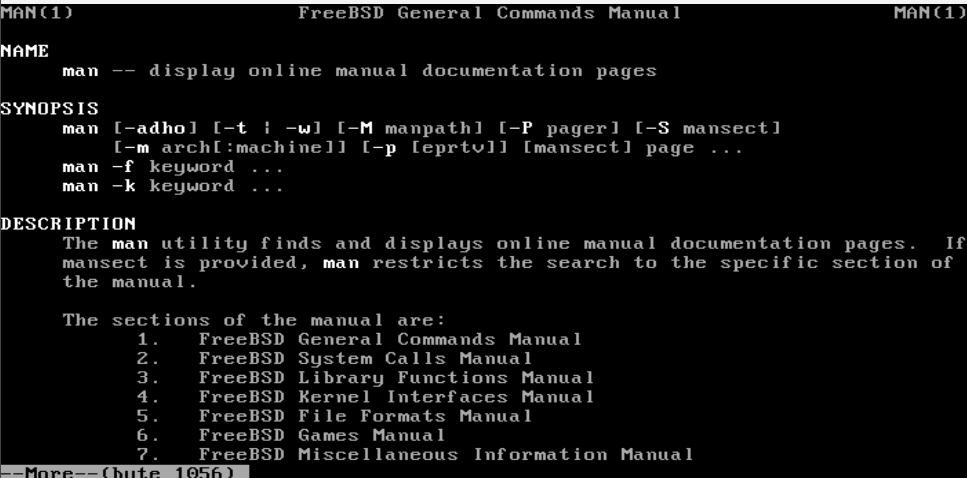
### 1.6

Το αποτέλεσμα της εντολής «man» είναι να μας ρωτήσει ποια manual page θέλουμε να δούμε.



### 1.7

Το αποτέλεσμα της εντολής «man man» είναι να μας εμφανιστεί το manual page για την εντολή «man».

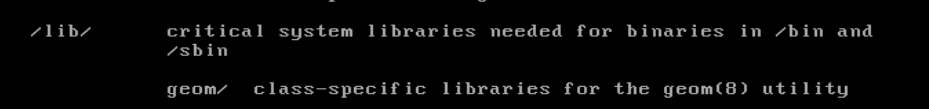


### 1.8

Το αποτέλεσμα της εντολής «man hier» είναι να μας εμφανιστεί η προκαθορισμένη ιεραρχία του συστήματος αρχείων του FreeBSD.(FreeBSD Miscellaneous Information Manual)

### 1.9

Ο κατάλογος lib/ περιέχει κρίσιμες βιβλιοθήκες συστήματος απαραίτητες για τους καταλόγους /bin και /sbin.



### 1.10

Περιέχει την πλειοψηφία υπηρεσιών και εφαρμογών του χρήστη.



### 1.11

Περιέχει προγράμματα του συστήματος και υπηρεσίες διαχείρισης θεμελιώδεις τόσο για περιβάλλοντα ενός χρήστη όσο και για περιβάλλοντα πολλαπλών χρηστών.



### 1.12

Στον κατάλογο /var/mail.



### 1.13

Περιηγούμαστε με τα εξής πλήκτρα: άνω/κάτω βελάκι, page up/down, home/end.

### 1.14

Με «slash → /<my word>»

### 1.15

Δεν χρειάζεται να διαβάσει ολόκληρο το input file για να ξεκινήσει, επομένως ξεκινάει πιο γρήγορα για μεγαλύτερα αρχεία. Επίσης επιτρέπει τόσο εμπρός κίνηση όσο και προς τα πίσω (forward, backward movement)

### 1.16

***hostname*** ---> PC.ntua.lab

### 1.17

***whoami*** ---> lab

### 1.18

***id*** ---> Ο αριθμός ταυτότητας (uid) του χρήστη lab είναι 1001.

### 1.19

***id*** ---> Ανήκει στην ομάδα χρηστών 0.

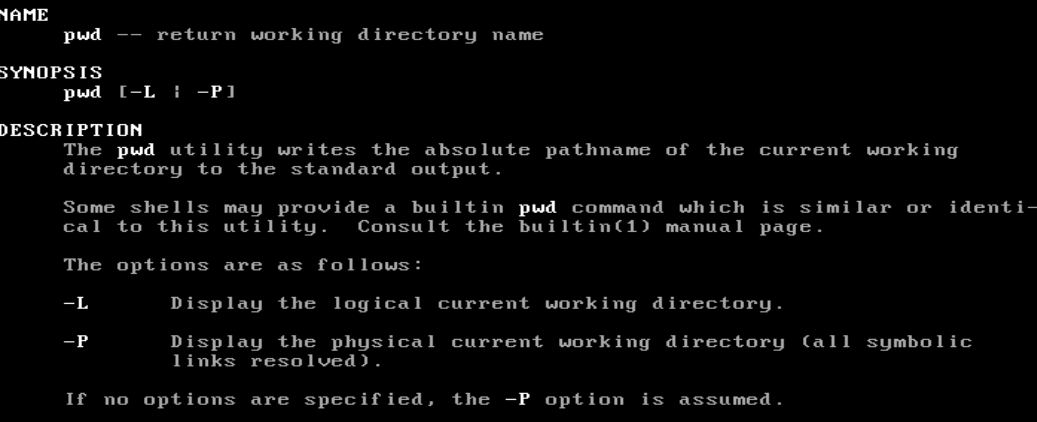
### 1.20

***pwd*** ---> /usr/home/lab

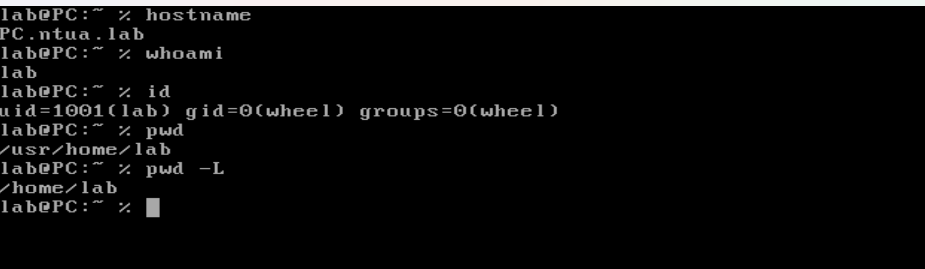
### 1.21

***pwd -L*** ---> /home/lab

Με την προσθήκη της επιλογής -L εμφανίζεται ο λογικός τρέχων κατάλογος(φάκελος) εργασίας ενώ στην 1.20 ερώτηση εμφανίζεται ο πραγματικός(physical) τρέχων κατάλογος(φάκελος) εργασίας.



1.21



1.16-1.21

### 1.22

root@PC:~#



### 1.23

***id*** ---> uid=0(root)

### 1.24

***id*** ---> 0(wheel),5(operator)

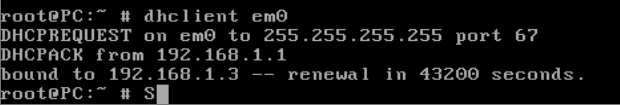
### 1.25

***id*** ---> gid=0(wheel)

### 1.26

***pwd*** ---> /root

### 1.27



IPv4 Address : 192.168.1.3+

### 1.28

***ifconfig*** ---> 2 διεπαφές em0 και lo0.

### 1.29

***ifconfig*** ---> MAC address : 08:00:27:72:31:bf

### 1.30

***ifconfig*** ---> Είναι 1Gbps (1000baseT).

### 1.31

***ifconfig*** ---> IPv4 address : 192.168.149.3

### 1.32

***ifconfig*** ---> Subnet Mask σε δεκαδική μορφή: 255.255.255.0

### 1.33

***ifconfig*** ---> MTU size: 1500 bytes.

### 1.34

IPv4 : 127.0.0.1

Subnet Mask : 255.0.0.0

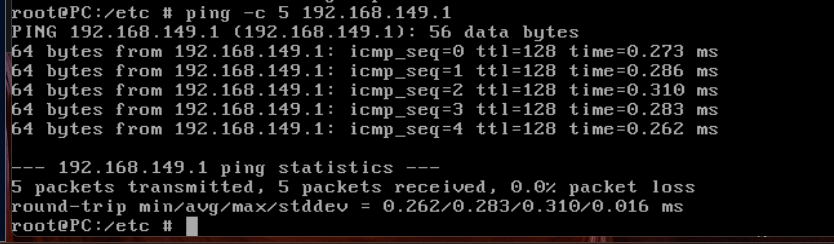
MTU size : 16384

### 1.35

Όχι, δεν έχουν οριστεί.

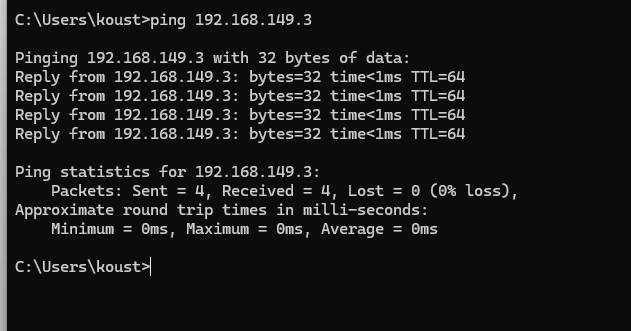
### 1.36

Ναι, απαντά.



### 1.37

Ναι, απαντά.



### 1.38

Εάν δεν οριστεί με κατάλληλη παράμετρο στέλνει αέναα ενώ στα Windows στέλνει 4 πακέτα by default.

# Άσκηση 2: Βασικές εντολές συστήματος αρχείων

### 2.1

***pwd*** ---> /usr/home/lab



### 2.2

**mkdir tmp***(working directory: /usr/home/lab)*

### 2.3

**cd tmp***(working directory: /usr/home/lab)*

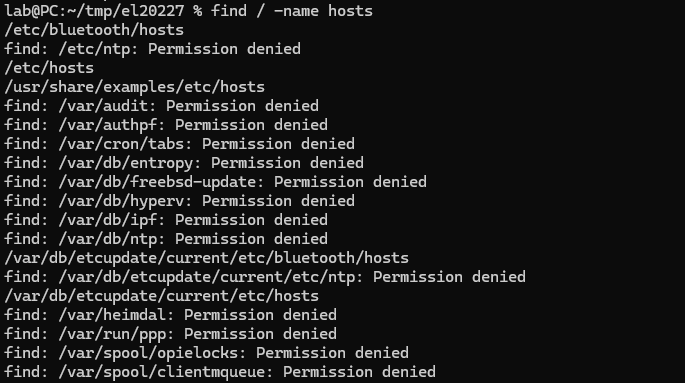
**mkdir el20227** *(working directory: /usr/home/lab/tmp)*

### 2.4

**cd el20227***(working directory: /usr/home/lab/tmp)*

### 2.5

**find / -name hosts** (*working directory: /usr/home/lab/tmp/el20227*)



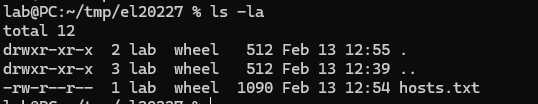
**cp /etc/hosts el20227** *(working directory /usr/home/lab/tmp)*

### 2.6

**mv hosts hosts.txt** *(working directory /tmp/el20227)*

### 2.7

***ls -la*** --->Επομένως, ο χρήστης έχει δικαιώματα ανάγνωσης και εγγραφής (rw), η ομάδα του χρήστη δικαιώματα ανάγνωσης (r), ενώ για οποιονδήποτε άλλον έχει πρόσβαση στο αρχείο, επιτρέπεται επίσης μόνο η ανάγνωση (r).



### 2.8

**touch test**

### 2.9

**touch .hidden**

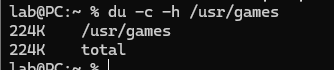
### 2.10

**ls -l /etc/services** ---> Size : 86128 bytes



### **2.11**

**du -h -c /usr/games** ---> Total size : 224 Kbytes

****

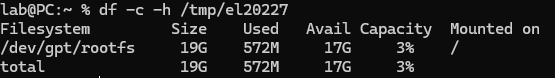
*(*[*https://ioflood.com/blog/du-linux-command/*](https://ioflood.com/blog/du-linux-command/)*)*

### **2.12**

Η διαφορά των 2 εντολών είναι πως η df -h εκφράζει το output στις μονάδες Byte, Kibibyte, Mebibyte, Gibibyte κ.λπ. (δυνάμεις τους 1024), ενώ η df -H στις μονάδες Byte, Kilobyte, Megabyte, Gigabyte κ.λπ. (δυνάμεις του 1000).

### **2.13**

**df -c -h /tmp/el20227** ---> Έχουμε 17 Gb ελεύθερο χώρο.



https://ioflood.com/blog/du-linux-command/

### **2.14**

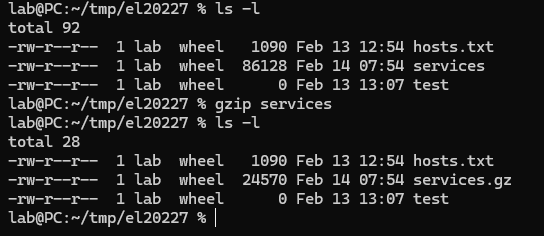
**cp /etc/services ./tmp/el20227**

### **2.15**

**ls -l** ---> pre-compression size : 86128 bytes

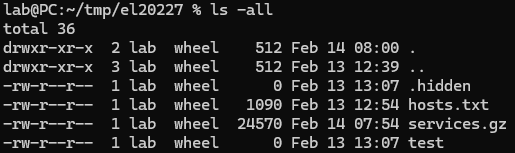
**gzip services** ---> <Compression>

**ls -l** ---> post-compression size : 24570 bytes



### **2.16**

**ls -all**



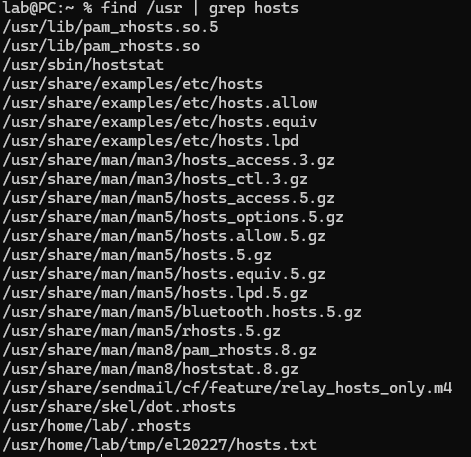
### **2.17**

**find /usr -name hosts** ---> Αρχεία με όνομα hosts.



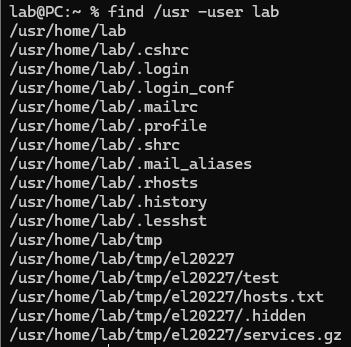
### **2.18**

**find /usr | grep hosts** ---> Αρχείο που περιλαμβάνουν στο όνομα του το string «hosts».



### **2.19**

**find /usr -user lab**



### 2.20

**rm hosts.txt .hidden services.gz test** (*working directory /usr/home/lab/tmp/el20227*)

### 2.21

**rm -r tmp/** (*working directory /usr/home/lab*)

# Άσκηση 3: Επεξεργασία κειμένου, ανακατεύθυνση εντολών

### 3.1

1. **cp /etc/hosts .** ---> Αντιγραφή ζητούμενου αρχείου (*working directory: /usr/home/lab*)
2. **vi hosts** ---> Για να ανοίξουμε το hosts με τον vi editor
3. **ESC** για να μεταφερθούμε σε command mode εντός του editor
4. **:%s /localhost/ntua-lab/ g** ---> Για να αλλάξουμε κάθε localhost με ntua-lab
5. **ESC** ---> Για να μεταφερθούμε σε command mode εντός του editor
6. **:q!** ---> Για να κλείσουμε το αρχείο χωρίς να αποθηκεύσουμε τις αλλαγές

### 3.2

**touch filelist && ls -l /etc > filelist**

### 3.3

**vi filelist** : Είσοδος στο αρχείο μέσω vi.

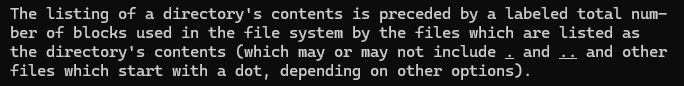
**ESC -> :1d** ---> διαγράφεται η πρώτη γραμμή

**:wq** ---> βλέπουμε πως μας εμφανίζεται στο τέλος του αρχείου η παρακάτω γραμμή:



### **3.4**

Διαγράψαμε τη γραμμή που έλεγε «total 812». Όπως διαβάζουμε από το documentation της ls, ο αριθμός αυτός αφορά το πλήθος των blocks που χρησιμοποιούνται από το filesystem από τα αρχεία που υπάρχουν στο directory που του δώσαμε ως όρισμα (στο /etc εν προκειμένω).



### **3.5**.

**wc filelist**

****

### **3.6**

Εκτελούμε την εντολή « **ls -l /etc | wc -l** » οπότε και μας εμφανίζεται ο αριθμός 106, και αφαιρώντας 1 για την πρώτη γραμμή που δεν αναπαριστά αρχείο, λαμβάνουμε το επιθυμητό πλήθος (μη κρυφών) αρχείων, ίσο με 105.

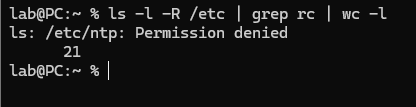


### **3.7**

1ος τρόπος :

**ls -l /etc | grep rc | wc -l** ---> Λαμβάνουμε ως αποτέλεσμα 15, αποτέλεσμα που αφορά αρχεία φακέλους/αρχεία που είναι ακριβώς μέσα στο /etc και όχι σε κάποιον υποφάκελο. 

**ls -l -R /etc | grep rc | wc -l** ---> Λαμβάνουμε ως αποτέλεσμα 21, αλλά και μήνυμα για αδυναμία πρόσβασης στο αρχείο /etc/ntp. Το αποτέλεσμα αυτό αφορά ολόκληρο το “δένδρο” καταλόγων και αρχείων κάτω από το /etc και όχι μόνο το πρώτο επίπεδο όπως πριν.



2ος τρόπος :

**ls -l /etc | grep --count rc**

**ls -l -R /etc | grep --count rc**

# Άσκηση 4 – Βασικές πληροφορίες συστήματος

### 4.1

**cat /var/run/dmesg.boot | grep CPU**

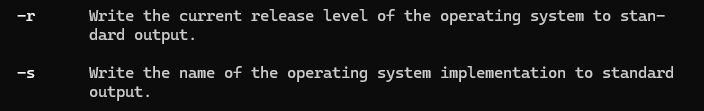
****

### 4.2

**cat /var/run/dmesg.boot | grep memory**

****

### 4.3



**uname –sr**



### **4.4**

**uptime** --->

****

### **4.**5

**service -e | wc**

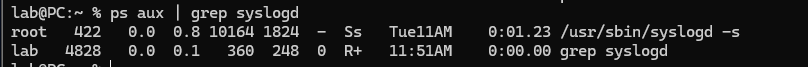


### **4.6**

**ps aux** ---> Εμφάνιση λίστας όλων των διεργασιών που τρέχουν στο σύστημα

### **4.7**

**ps aux | grep syslogd**

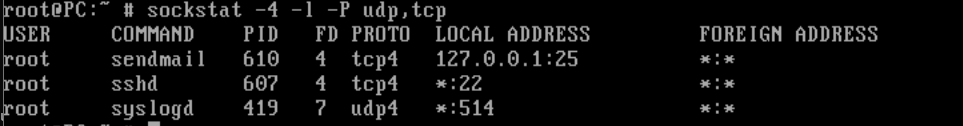
****

### **4.8**

**netstat -s -p tcp | awk '$1 != 0'**

### **4.9**

**sockstat -4 -l -P udp,tcp**

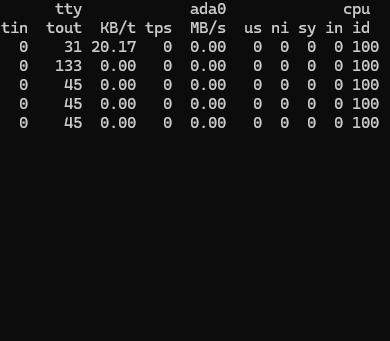


### **4.10**

**top** ---> Eμφάνιση σπουδαιότερων επεξεργαστικά processes.

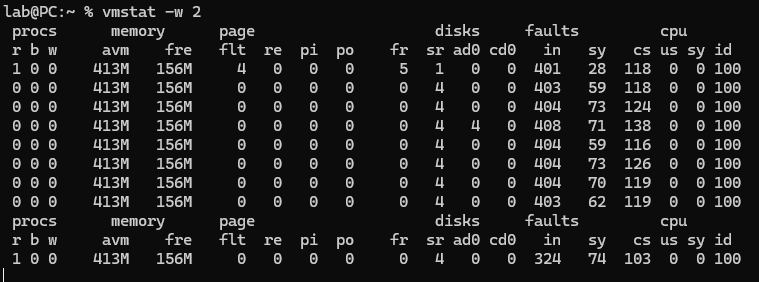
### **4.11**

**iostat ada0 –w 1**

****

### 4.12

**vmstat -w 2** --->



# Άσκηση 5 – Πρόσβαση ως root

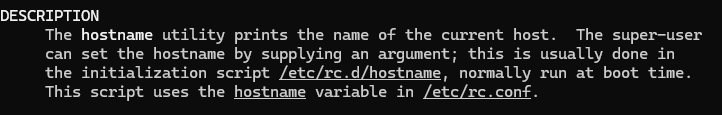
### **5.1**

Για λόγους ασφαλείας απαγορεύεται η πρόσβαση ως root μέσω ssh, καθώς εάν επιτρεπόταν θα μπορούσε κάποιος να δοκιμάσει με brute force πιθανούς κωδικούς μέχρι να καταφέρει να συνδεθεί με πλήρη δικαιώματα.

Χρησιμοποιώντας τις εντολές cat, ping, who, w, hostname και su και απαντήστε στα παρακάτω ερωτήματα καταγράφοντας την πλήρη σύνταξη των εντολών που χρησιμοποιήσατε:

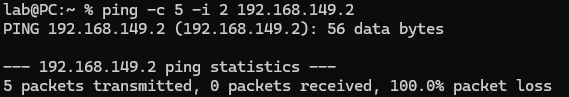
### **5.2**

Με την εντολή « **hostname** » βλέπουμε πως το όνομα του εικονικού μηχανήματος είναι «PC.ntua.lab». Από το documentation της hostname, διαβάζουμε ότι το hostname μπορεί να το αλλάξει μόνο ο superuser δίνοντας κατάλληλο όρισμα στο script /etc/rc.d/hostname κατά το boot time, επομένως ο lab user δε μπορεί να αλλάξει το όνομα σε «virtualmachine» .



### **5.3**

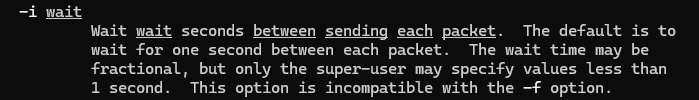
**ping -c 5 -i 2 192.168.149.2** ---> Success



### **5.4**

**ping -c 5 -i 0.1 192.168.149.2** ---> Fail : Για χρόνους ενδιάμεσης παύσης μικρότερους από 1 δευτερόλεπτο έχει δικαίωμα μόνο ο root.





### **5.5**

Μπορούμε να επιτύχουμε τα παραπάνω όντας root user.

### **5.6**

**who** ---> Χρήστες root και lab



### **5.7**

Εκτελώντας την εντολή « **su** », εάν έχουμε ήδη δικαιώματα διαχειριστή δε γίνεται τίποτα, ενώ εάν δεν έχουμε τέτοια δικαιώματα μας ζητείται κωδικός, ώστε να γίνουμε root.



### **5.8**

**cat /var/log/auth.log**

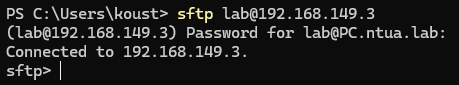


### **5.9**

Όντας root χρήστης στο εικονικό μηχάνημα, εκτελούμε « **su lab** », οπότε και γινόμαστε απλός χρήστης χωρίς αυξημένα δικαιώματα χωρίς να μας ζητηθεί κωδικός κατά την αλλαγή. Αυτό δικαιολογείται από το γεγονός πως ο root είχε ήδη περισσότερο δικαιώματα από τον lab, οπότε τα δικαιώματα του lab στα οποία θα έχει πρόσβαση πλέον ο root είναι υποσύνολο αυτών που ήδη είχε, επομένως δε τίθεται θέμα ασφαλείας.



# Άσκηση 6 – Μεταφορά αρχείων



### **6.1**

**ls -all**

### **6.2**

**get -r lab c:\users\koust\downloads\temp**

### **6.3**

**get /etc/hosts c:\users\koust\downloads\temp**

get /etc/rc.conf c:\users\koust\downloads\temp

### **6.4**

Όντας στο /usr/home/lab του remote μηχανήματος, εκτελούμε την εντολή « **mkdir tmp** »

### **6.5**

**put -r c:\users\koust\downloads\temp /usr/home/lab/tmp** 

### **6.6**

Όχι γιατί περιέχει αρχεία.

### **6.7**

Όντας στον φάκελο /usr/home/lab/tmp, εκτελούμε την εντολή « **rm \*** » και διαγράφονται όλα τα αρχεία που περιέχονται στον φάκελο tmp στο εικονικό μηχάνημα.

### **6.8**

Όχι.

### **6.9**

Διαγράψαμε και τα κρυφά αρχεία με « **rm .\*** »

### **6.10**

**rmdir temp**

**cd ..**

**rmdir tmp**

### **6.11**

**get -r /etc c:\users\koust\downloads\etc**

### **6.12**

Η μεταφορά δεν ολοκληρώνεται, καθώς κατά το κατέβασμα των αρχείων, προηγείται το άνοιγμα καθενός εξ αυτών (open(“etc/filename”), το οποίο και αποτυγχάνει σε ορισμένα λόγω περιορισμένων δικαιωμάτων.

### **6.13**

**put -r c:\users\koust\downloads\etc /usr/home/lab**

### **6.14**

**rename etc tmp**